UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF PENNSYLVANIA

BESSEMER SYSTEM FEDERAL CREDIT UNION, Plaintiff, vs. FISERV SOLUTIONS, LLC, f/k/a FISERV SOLUTIONS, INC., and FISERV, INC., Defendants.	Case No. 2:19-CV-00624-RJC

DEFENDANTS' RESPONSE TO BESSEMER'S OBJECTIONS TO SPECIAL MASTER'S REPORT AND RECOMMENDATION

INTRODUCTION

The Special Master has spent more than a year familiarizing himself with this case, evaluating the parties' discovery disputes, and facilitating the exchange of discovery through mediated meet and confer sessions. The disputes that remain were exhaustively briefed–92 pages of letter submissions to the Special Master, in addition to the original briefing on these motions. After a two-hour hearing, the Special Master issued a thorough and well-reasoned report and recommendation. (Dkt. 209.) Applying Rule 26's relevancy and proportionality standards, the Special Master found that the scope of discovery, as framed by the parties' pleaded claims and defenses, should be limited to the issues concerning the parties' business relationship and the products and services that Fiserv actually provided to Bessemer.

The Court will recall that it was Bessemer that pushed for appointment of a special discovery master in the first place, insisting that would expedite matters and conserve resources. (Dkt. 132.) Fiserv preferred a special master limited to ESI issues, predicting that Bessemer would object to any adverse discovery ruling and require this Court to resolve most discovery issues anyways. (Dkt. 141.) Precisely that has come to pass. Despite the Special Master's substantial investment of time and detailed analysis, Bessemer objects to **nearly** every one of his recommendations. Apparently, all of them are wrong.

Yet, by and large, Bessemer fails to identify specific errors requiring deviation from the Special Master's recommendations. Instead, Bessemer resorts to generality and hyperbole, asserting that the Special Master has "artificially" limited discovery. Bessemer repeats the well-worn arguments it has been making for years, ignoring entirely Fiserv's substantial document production and failing to detail any specific, relevant document or piece of information that Fiserv has not produced. Fiserv has produced some 26,000 pages of documents and substantially completed document discovery. The Master Agreement limits Bessemer's contract damages to

approximately $27,000; Fiserv has spent more than 20 times that amount collecting and producing responsive materials. (Dkt. 48 ("SAC"), Ex. 2 § 7; Dkt. 218-6 at 7.)

Still, Bessemer demands more. Yet, rather than clearly identify what is supposedly "missing," Bessemer invokes "associational standing" (which this Court has plainly rejected), its "fraud" claims (which are substantively and temporally narrow), and its demand for "punitive damages" (on its contract claims, no less) as justification for enterprise-wide discovery. This is a fishing expedition, plain and simple. Bessemer wants discovery (and proportionality) to be a one-way street, demanding remarkably broad discovery about products and services that Bessemer never received and the (other) customers who used those products and services, while completely resisting discovery on the so-called "security review" (even in the face of the Court's directive that discovery was necessary) and invoking its status as a "small credit union" at every turn to deny Fiserv discovery about its 90-page, 336-paragraph Second Amended Complaint. The Special Master properly applied Rule 26 to reject such a one-sided framework. This Court should as well and should adopt the Special Master's recommendations in full.

BACKGROUND

On June 8, 2022, the Court appointed Mr. Shepard as Special Master to oversee discovery and resolve the parties' disputes. (Dkt. 195.) Over the past year, the parties and the Special Master have committed substantial resources to the process. Beyond the twelve briefs addressing these motions, the Special Master conducted five status conferences and mediated meet and confer sessions, the parties submitted twelve letter motions and position statements, and the Special Master conducted multiple hearings, most recently on May 16, 2023, regarding these disputes.

Apart from the discovery disputes now before this Court, the parties have made substantial progress in written and document discovery. On December 13, 2022, the Special Master instructed the parties to commence document production and, subsequently, the parties exchanged rolling

productions for approximately two months. To date, Fiserv has produced almost 9,000 documents, consisting of more than 26,800 pages. Although one would not know it from Bessemer's objections, the discovery posture of this case has changed markedly from when these motions were first filed ***in December of 2021 and January of 2022.*** Most importantly, Fiserv has substantially completed document discovery (and conducted the first deposition in this case) and believes that Bessemer, too, is nearing substantial completion.

Trafficking in abstraction, Bessemer pretends that Fiserv's production is somehow inadequate and "artificially" limited. But Fiserv has made an exhaustive production with respect to its contractual relationship with, and products and services provided to, Bessemer. Fiserv has produced documents about those products and services generally (not just Bessemer's experience with them) and Fiserv's information security policies and procedures, including a decade's worth of independent security audit reports for those systems; meeting minutes about those products and services;[1] documents reflecting updates, development, and testing with respect to those systems; and security policies and plans that govern the products and services Bessemer received. Specifically, and as explained in Fiserv's responses, Fiserv has produced:

- Annual independent SOC Audit Reports from 2012-2020 for Charlotte and 2012-2019 for Virtual Branch—the core products and services that Bessemer received under the Master Agreement.
- Its information security plan and security policies that apply to the products and services Bessemer received, along with documents detailing Fiserv's general security practices.
- Nearly 500 service-related tickets for Bessemer alone, which range from issues about which Bessemer complained to routine requests for a password reset or instructions on performing a particular transaction.

[1] Those documents, like many other documents Fiserv has produced, are not specific to Bessemer and cover general topics relating to Charlotte and Virtual Branch, including testing and development, bugs and defects, reports and resolutions of other customer complaints, security testing, and other topics relating to the account processing system and online banking platforms Bessemer used.

- Charlotte and Virtual Branch Meeting Minutes dating as far back as 2009 and through 2019, irrespective of whether such documents expressly reference Bessemer.

- Over 600 documents from 2014 to 2019 relating to updates and releases for Sellstation—the application that Bessemer used to interact with Charlotte—that include information on updates and releases for virtually every Charlotte customer.

- Security incident reports relating to issues that may have impacted Bessemer or another Charlotte or Virtual Branch customer. Those documents specifically list potentially impacted clients. (The only ticket that relates solely to Bessemer is that created for Bessemer's brute force attack. For the others, Bessemer is just one of multiple clients identified.)

- The master customer file for Bessemer that contains correspondence between the parties from on or around 1980 through approximately 2010.

- Hundreds of emails relating to complaints by Bessemer and Fiserv's analysis and resolution of those complaints.

- Hundreds of documents relating to the incidents Bessemer characterizes as a "data breach" and the "security review," including documents relating to Fiserv's investigation and response to those events.

- Documents from Richard Reynolds (who wrote the email that is the basis for Bessemer's fraudulent inducement claim) relating to Bessemer, Virtual Branch, and Authentication/FFIEC standards, without any limitation to Bessemer and back to 2005, the earliest date that Mr. Reynolds' email was available.

Fiserv also conducted additional searches to identify and produce the limited additional documents that the Special Master recommended be produced. Bessemer's claim that Fiserv or the Special Master's report and recommendation have "artificially" limited discovery lacks any factual basis.

Fiserv has now completed document discovery, subject to limited categories identified in the R&R, this Court's order approving the R&R, and good faith follow-up on discrete issues. The only document discovery Fiserv requires from Bessemer, aside from discrete issues identified in discovery correspondence, is that relating to Bessemer's security review, which the Special Master recommended be produced. Fiserv is prepared (and eager) to complete fact discovery by the September 25, 2023, and has begun depositions to meet the current deadline.

ARGUMENT

To Bessemer, discovery is largely a one-way street. Bessemer believes the Special Master erred by denying enterprise-wide discovery concerning all of Fiserv's products, services, and customers spanning over a decade in light of Bessemer's narrow tort claims and demand for punitive damages. When it comes to discovery required of Bessemer, however, it advocates for "proportionality" and claims that the Special Master erred by requiring Bessemer to produce discovery relating to its brute force attack. Bessemer has declined every invitation to reconcile this stunning lack of consistency or to identify specifically, given Fiserv's fulsome productions, what "more" discovery it needs and why. Bessemer's general and repeated complaint that discovery has been "artificially narrowed" is no basis to disturb the Special Master's well-reasoned R&R.

I. THE SPECIAL MASTER APPROPRIATELY DENIED BESSEMER'S REQUESTS FOR ENTERPRISE-WIDE DISCOVERY.

After hearing the parties' arguments and reviewing their voluminous submissions, the Special Master recommended denying (a) Bessemer's Motion to Compel Production of Documents Unrelated to Bessemer and/or Other Fiserv Clients, Systems and Services, (b) Bessemer's Motion to Compel Documents and Information Related to Security Audit and Communications or Notices Regarding Security Deficiencies or Complaints Related to Fiserv Products, (c) Bessemer's Motion to Compel Production of FFIEC Reports, and (d) Bessemer's Motion to Compel Fiserv to Provide a Privilege Log for Communications After June 30, 2019. (Dkt. 209, Section III (A)(1), (3), (5) and (7).) Bessemer objects to all of these recommendations.

The common thread is Bessemer's unwarranted (and expensive) fishing expedition for something Bessemer thinks it can use to paint Fiserv as a bad actor that has committed "fraud" or should be "punished" with punitive damages. Bessemer sees this case as some sort of quasi-regulatory enforcement action or consumer class action implicating Fiserv's entire business and

relationships with its thousands of customers. Yet, the Court long ago rejected that notion along with Bessemer's claim that it had "associational standing" to prosecute claims on behalf of its members. This is, at its core, a breach of contract case with two (narrow) fraud theories sprinkled in for good measure. Bessemer is not a regulator and this is not a class action. As the Special Master recognized, the claims Bessemer actually pleaded do not merit enterprise-wide discovery.

A. BESSEMER'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS UNRELATED TO BESSEMER OR THE PRODUCTS AND SERVICES IT RECEIVED

The Special Master recommended denying Bessemer's request to expand the scope of discovery to include "any alleged or reported security deficiency, service complaint, data breach, alleged system deficiencies or client dissatisfaction relating to any other Fiserv customer and/or any Fiserv service or system." (Dkt. 209 at 9.) Bessemer contends that adopting this recommendation would "artificially" narrow discovery and deprive Bessemer of evidence necessary for its fraudulent inducement claim and punitive damages demand. (Dkt. 216 at 2-5.) That argument ignores the narrow factual and temporal bases for Bessemer's fraudulent inducement claim and the significant discovery Fiserv has already produced.

Bessemer's fraudulent inducement claim is based on an email dated February 27, 2012, to Bessemer's former CEO, Linda Gregory, from its Fiserv account executive, Richard Reynolds:

From: Reynolds, Richard <Richard.Reynolds@fiserv.com>
Sent: Monday, February 27, 2012 9:16 AM
To: Linda Gregory
Subject: RE: FFIEC Authentication

There shouldn't be a problem with this. I think VB is up to their requirements.

From: Linda Gregory [mailto:lgregory@bessfcu.com]
Sent: Wednesday, February 22, 2012 12:51 PM
To: Reynolds, Richard
Subject: FFIEC Authentication

Hi Richard - my NCUA examiner is hitting in March - with respect to the January 2012 updates by FFIEC to the authentication process, how does our Virtual Branch match up to their expectations? Anything I need to be aware of or concerned about? Thanks, Linda

(SAC, Ex. 3.) Bessemer alleges that Mr. Reynolds' statement –"there shouldn't be a problem with this. I think VB is up to their requirements"– was a knowingly false misrepresentation that induced Bessemer to enter into the Master Agreement in July 2014, ***two and a half years later***.

Bessemer's fraudulent inducement claim is based on one statement, made by one Fiserv employee (Mr. Reynolds), relating to one product (Virtual Branch).[2] Bessemer asserts that this email opens the door to enterprise-wide discovery with respect to all of Fiserv's information security and authentication processes, for all products and services, from their development through the present. Bessemer attempts to support this remarkable position by asserting that enterprise-wide discovery is necessary to show that Fiserv—***as an enterprise***—had knowledge of the alleged falsity. This ignores the law, namely that "the requisite mental state of scienter must be found within the mind of an employee who either made, or participated in the making of, such a statement." *City of Roseville Emps. Ret. System v. Horizon Lines, Inc.*, 686 F.Supp.2d 404, 425 (D. Del. 2009). The relevant inquiry for the scienter element here is Mr. Reynold's knowledge. Courts reject the "collective scienter" theory that Bessemer advances. *Nordstrom, Inc. v. Chubb & Son, Inc.*, 54 F.3d 1424, 1435 (9th Cir. 1995) ("Federal argues that it is conceivable that a jury would find that none of the named directors and officers had the requisite intent, but that the corporate entity had such intent under a theory of 'collective scienter….' However, there is no case law supporting an independent 'collective scienter' theory.").

[2] The description of this communication in Bessemer's objection takes some significant liberties, implying a far more extensive communication: "Bessemer's fraudulent inducement claim is predicated on Fiserv's misrepresentations regarding the existence and nature of security controls it placed on its Virtual Branch and Charlotte systems." (Dkt 216 at 4.) Bessemer also asserts that "Fiserv falsely represented that its Virtual Branch authentication process had security controls that were complaint with FFIEC cybersecurity requirements." (*Id*.) In response to Fiserv's discovery requests, Bessemer has conceded that this email constitutes the entire basis for its claim – it has neither identified nor produced any other email or other communications on the subject. The email is all there is.

With respect to the relevant discovery period, the Special Master concluded that discovery back to 2011, a year before Mr. Reynolds sent his email, was appropriate. Bessemer objects to this as "arbitrary" and demands discovery back to the initial creation of the Virtual Branch product in the 2000's. That argument ignores the narrow factual and temporal parameters of Bessemer's claims, as framed by Mr. Reynolds' email. On its face, the email addresses only whether Virtual Branch complied with the FFIEC's "January 2012 updates." Mr. Reynolds responded that he thought Virtual Branch did. If he lied (and he did not), the relevant evidence would relate to that update (in 2012) and whether Virtual Branch complied with that update (in 2012). The Special Master's recommendation acknowledges the possibility that communications relating to those issues could have occurred earlier and ordered discovery for the previous year as well. Bessemer's attempt to recharacterize this narrow claim as implicating whether Virtual Branch always complied in every respect with all FFIEC requirements, past and present, fails. That is not what Bessemer has pleaded (or could plead consistent with Rule 9(b)). The claim Bessemer did plead provides no basis for unlimited, enterprise-wide discovery.

Discovery on this claim has not been artificially narrowed in any way. To the contrary, Fiserv has performed exhaustive efforts to identify potentially relevant documents and material in a good faith effort to resolve this dispute. Based on the Special Master's guidance during a status conference on March 7, 2023, and well before Bessemer filed its letter motion, Fiserv attempted to resolve this issue by retrieving Mr. Reynolds' back-up email files, which date back to 2005, and searching those emails using the same (500) search terms used for other email searches ***and*** applying additional, broad terms relating to Virtual Branch, FFIEC, and authentication, without

limiting those terms to Bessemer, and producing all responsive documents.[3] (Dkt. 218, Ex. F at 11-12.) Bessemer's objection, of course, makes no mention of these additional efforts, which were detailed extensively in Fiserv's submission to the Special Master (*id*), and instead myopically repeats its "artificially limited" mantra.

Fiserv has diligently performed its discovery obligations, at great expense, and made reasonable and proportional efforts (and then some) to identify, retrieve, and produce documents potentially relevant to Bessemer's fraudulent inducement claim. That claim is factually and temporally narrow and provides no basis for the enterprise-wide discovery that Bessemer demands.

B. BESSEMER'S MOTION TO COMPEL SECURITY AUDITS

Bessemer first filed an ill-defined motion for what it calls "security audit documents," a term not defined in the Master Agreement or Bessemer's motion, on January 31, 2022, long before the parties had produced any documents. (Dkt. 161.) Fiserv responded, highlighting the incredible breadth of the requests and noting the prematurity of the motion. (Dkt. 173.) While this motion was pending, the Special Master resolved the parties' dispute about a protective order and directed the parties to commence document production. Fiserv complied and, among many other documents, produced the SOC Audit reports for the systems (Charlotte and Virtual Branch) Bessemer used under the Master Agreement, security policies and plans applicable to those systems generally, and security incident reports, service tickets, meeting minutes, and emails relating to Bessemer, the systems it used, and other customers utilizing such systems. Whatever "security audit documents" means, Fiserv has made a reasonable and proportional production of such documents.

[3] Fiserv applied the following additional searches: (FFIEC AND "virtual branch"); (FFIEC AND VB); (Authenticat* AND "virtual branch"); and (Authenticat* AND VB).

Completely ignoring what Fiserv produced, Bessemer rotely renewed its motion for "security audits" on March 22, 2023. Bessemer's abstract discussions about discovery ignore that the parties are now in a fundamentally different posture. After receiving the thousands of pages of documents that Fiserv has produced (which Bessemer has had for months), Bessemer must present competent evidence that Fiserv has not conducted a reasonable inquiry, search for, and production of responsive documents. *See Enslin v. Coca-Cola Co.*, 2016 WL 7042206, at *3 (E.D. Pa. June 8, 2016); *Scott C. v. Bethlehem Area Sch. Dist.*, 2002 WL 32349817, at *1 (E.D. Pa. July 23, 2002). Bessemer's hypothetical (and often inaccurate) discussions of its needs for unbridled enterprise-wide discovery come nowhere close to satisfying this burden. After reviewing Fiserv's explanation of the documents it has already produced, the Special Master agreed, recommending that the motion be denied, except as to a subset of documents from 2011 and 2012 (to which Fiserv has not objected). (Dkt. 209 at 7-8.)

Bessemer of course objects, but does not contest that Fiserv has made a fulsome production of "security" documents relating to Bessemer and the products and services that Bessemer actually used. Here, again, Bessemer demands enterprise-wide discovery, insisting that its demand for punitive damages and fraudulent inducement claim make its remarkable demands both relevant and proportional. They do not. As explained above, Bessemer's fraudulent inducement claim relates to a single email from 2012 about a single product (Virtual Branch) and updates to 2012 FFIEC standards. The enterprise-wide "audit" documents that Bessemer demands have no conceivable relationship to that claim. Indeed, Bessemer does not even attempt to suggest that, much less explain how, its demands could be considered proportional.

Bessemer's reliance on its punitive damages demand fares no better. As Fiserv has explained (Dkt. 173 at 12-13; Dkt. 218, Ex. F at 3-5), Bessemer's claims relating to Fiserv's

information security practices are contract claims, governed by the Master Agreement and for which Bessemer expressly disclaimed punitive damages. (SAC, Ex. 2 at § 7.) Bessemer never explains why discovery about a breach of contract claim and the two isolated events that form the basis for that claim—a 2016 incident where four member records were inadvertently sent to a different credit union client and a 2017 incident where an incorrect return address was placed on certain account verifications—open the door to an unfettered "audit" of Fiserv's entire product line and any security incident over the last decade. They don't. Given the Master Agreement's $27,000 limitation of liability, it is no surprise that Bessemer is silent about proportionality.

Instead, Bessemer pretends that this case involves wide-spread data breaches impacting countless consumers. But, as framed by Bessemer's own allegations in the SAC, it is not.[4] Bessemer offers only naked assertions of unknown and unidentified security vulnerabilities, which are insufficient even to state a claim, *see e.g.*, *Bohnak v. Marsh & McLennan Cos., Inc.*, 2022 WL 158537, at *6 (S.D.N.Y. Jan. 17, 2022); *Willey v. J.P. Morgan Chase, N.A.*, 2009 WL 1938987, at *9 (S.D.N.Y. July 7, 2009), much less to justify highly-invasive, enterprise-wide discovery. Indeed, even in real data breach cases, courts have taken the same approach as the R&R and limited discovery to the particular systems that impacted the plaintiff, refusing discovery across all of defendant's platforms. *In Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 185 (M.D. Tenn. 2014) ("Discovery of other parts of Genesco's computer system that were not the bases for the fines and assessments would not lead to discovery of relevant information about the bases for Visa's fines and assessments."). Likewise, courts have rejected similar far-reaching requests to

[4] Bessemer has admitted that it possesses no facts that would support such a claim. (Dkt. 173 at 12-13.) Specifically, Bessemer has admitted that it is not aware of any incident in which acts or omissions of Fiserv have resulted in identity theft, that none of its members has reported any incident in which the acts or omissions of Fiserv have resulted in identity theft, and that no member reported that their account had been used or accessed fraudulently in response to correspondence sent in April 2019, soliciting precisely that information. (Bessemer Resp. to RFA Nos. 33-35.)

extend the relevant time period for discovery beyond what is necessary for the claims actually pleaded. *In re Brinker Data Incident Litig.*, 337 F.R.D. 424, 425 (M.D. Fla. 2020).[5]

The thrust of the claims Bessemer has actually pleaded is that the services and products it received from Fiserv were deficient. That will not avoid the liability limitation or permit punitive damages, so Bessemer is on a fishing expedition for more. Rather than prosecute its contract claims, Bessemer hopes to discover any incident, at any time, involving any Fiserv product or customer, to argue that Fiserv has been "reckless and indifferent." Courts (rightly) do not permit plaintiffs to prosecute hypothetical claims relating to unidentified incidents on behalf of unidentified consumers in a quest for punitive damages. *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408 (2003) ("Due process does not permit courts, in the calculation of punitive damages, to adjudicate the merits of other parties' hypothetical claims against a defendant under the guise of the reprehensibility analysis."); *see also Fung-Schwartz v. Cerner Corp.*, 2020 WL 4927485, at *9 (S.D.N.Y. Aug. 21, 2020) (rejecting discovery on incidents unrelated to claims and holding that "to permit punishment for injuring a nonparty victim would add a near standardless dimension to the punitive damages equation."). Bessemer has failed to show that the Special Master's determination that Fiserv has produced the security information that is relevant to Bessemer's claims conclusion is incorrect in any way. The Court should overrule the objection.

C. "DRAFT" FFIEC EXAMINATION REPORTS

The Special Master recommended denying Bessemer's request for FFIEC examination reports, concluding that Bessemer should obtain such reports from the FFIEC. (Dkt. 209 at 10-11.)

[5] "Plaintiffs argue that multi-factor authentication ("MFA") was installed in 2017—allegedly three years late—but not implemented, enabling the hackers to gain access, and, therefore, Plaintiffs should be entitled to information from 2014 (the year MFA should have been installed). However, this example, and all the others listed by Plaintiffs, are unpersuasive. Ultimately, if Brinker was violating industry standards or its own IT and data security policies in 2018, it does not greatly matter how long those violations were ongoing."

Bessemer objects, making the completely new request (never made to Fiserv or the Special Master) that Fiserv produce ***draft*** FFIEC examination reports. That "objection" makes no sense.

First, Bessemer never filed a motion seeking FFIEC reports. Rather, in response to Bessemer's request for broad discovery relating to its fraudulent inducement claim, Fiserv simply explained that potentially relevant information is not in Fiserv's possession, including FFIEC reports concerning Virtual Branch, and that Bessemer expressly agreed to obtain such reports directly from the FFIEC in Section 10(a) of the Master Agreement. This issue was briefly discussed at the hearing, and Fiserv's counsel later provided the Special Master with the authority prohibiting Fiserv's disclosure of FFIEC reports. As a result, the Special Master ruled that Bessemer must obtain these reports from the FFIEC.

Second, FFIEC reports (and "drafts") are prepared by the FFIEC, not Fiserv. If Bessemer now wants draft FFIEC reports, it must request those from the FFIEC as well. Had Bessemer, after a year of meeting and conferring with Fiserv, ever asked for "draft" FFIEC reports before, Fiserv would have made this clear then. There is no valid "objection" here to consider.

D. BESSEMER'S MOTION TO COMPEL A PRIVILEGE LOG FOR COMMUNICATIONS AFTER JUNE 30, 2019

In January 2022, Bessemer moved for an order compelling Fiserv to log privileged communications after June 30, 2019, and through the conclusion of litigation. The Special Master recommended that the motion be denied, finding that the request would unnecessarily burden both parties with "little or no benefit." (Dkt. 209 at 6.) Bessemer's objection contends that a supposedly ongoing dispute about "ownership" requires Fiserv to log years of privileged communications. Common sense and proportionality dictate that the Court overrule the objection.

Bessemer filed its complaint in April 2019, and completed its transition to its new processing vendor on May 31, 2019. As part of that process, Bessemer made demands for certain

archived data for which the Master Agreement required Bessemer to pay. Bessemer never paid, but Fiserv provided the records anyways. After Bessemer had some technical issues accessing the documents, it sought a TRO, which Judge Horan denied, ordering the parties to work together and resolve the issue. They quickly did, and Bessemer received the remaining records by June 30, 2019. Given its preservation obligations, Fiserv has maintained archived copies of those records. Bessemer's deconversion was complete by June 30, 2019, which Fiserv suggested, and the Special Master agreed, is the right cut-off date for privilege logs. (Dkt. 173 at 19 (collecting cases).)

Bessemer has attempted to manufacture a "continuing" dispute that it says requires Fiserv to log privileged communications until this case ends. Years ago, in response to a generic demand from Bessemer's counsel for "all" Bessemer's records and information, Fiserv's counsel recited the Master Agreement's definitions of "Client Information" and "Fiserv Information." Since that time, Bessemer has asserted (incorrectly) that Fiserv "claims ownership" of Bessemer's "Client Information," and made this the subject of bailment and declaratory judgment claims. Fiserv has never claimed "ownership" of these records and has attempted to disabuse Bessemer of this notion many times, to no avail, making clear that Fiserv is prepared (and eager) to destroy all remaining records when this litigation ends. Bessemer will not take yes for an answer, preferring the fight.

Even if a "dispute" existed, however, it would provide no grounds to require Fiserv to log all of its privileged communications for the last four (and unknown future) years of this litigation. The burden is both palpable and disproportional, and Bessemer cannot articulate any conceivable benefit (other than imposing an expensive burden on Fiserv). To the extent there is an ownership dispute here, it is contractual and dictated by the terms of the Master Agreement. Privileged communications years after the "dispute" arose would have no bearing on what the Master

Agreement says about ownership. Bessemer's "continuing dispute" argument is absurd and would preclude a privilege log cut off in every case involving a property dispute. That is not the law.

II. THE SPECIAL MASTER APPROPRIATELY ORDERED DISCOVERY WITH RESPECT TO THE SECURITY REVIEW.

A. FISERV'S MOTION TO COMPEL INFORMATION RELATING TO THE SECURITY REVIEW.

Bessemer objects to the R&R granting in part Fiserv's motion to compel discovery relating to the security review. (Dkts. 138-9, 152.) In September 2018, Bessemer orchestrated a brute force cyberattack on Fiserv's online banking platform (what Bessemer calls the "security review"). The events surrounding the security review are central to Bessemer's claims and Fiserv's counterclaims. Alleging that the security review uncovered vulnerabilities, Bessemer devotes three pages of the SAC to allegations about it. (SAC ¶¶ 58-67.) As the Court is aware, Fiserv's counterclaims allege that the security review breached the Master Agreement. Denying Bessemer's motion to dismiss that claim, the Court expressly held that "[d]iscovery is necessary before this Court can ascertain the actions leading up to, and involved in, the 'security review,' the motivations behind it, and the information that was ultimately accessed as a result of the 'review.'" (Dkt. 120 at 19-20.) Bessemer has nonetheless resisted all discovery about the security review.

The R&R carefully analyzed the parties' competing positions and found a middle ground. Agreeing (consistent with the Court's earlier ruling) that the security review is relevant, the Special Master concluded that the subject is discoverable. Yet, the Special Master acknowledged the possibility that some of what Fiserv seeks, such as communications between the security reviewer and Bessemer's counsel, might be privileged and directed Bessemer to log documents and communications over which it asserts a privilege. (Dkt. 209 at 15-19.) Neither party got everything it wanted; only Bessemer has objected.

Bessemer's objection (again) tries to reframe the security review as a post-litigation, after-the-fact incident analysis performed only for litigation purposes and about which Bessemer "scrupulously" maintained confidentiality. Specifically, Bessemer now contends that the security reviewer is a consulting expert who was hired by counsel after it "commenced litigation." That argument does not square with the chronology, the SAC's allegations, or Bessemer's (many) prior representations to Fiserv and the Court about the purpose of the security review.

In April 2018, Bessemer served a praecipe writ of summons but not a complaint. There was a lawsuit, but no allegations or claims at that time. In September 2018, Bessemer commissioned and performed the security review – a brute force attack on Fiserv's systems. ***Seven months later***, in April 2019, Bessemer first filed its complaint, making a host of allegations about the security review, its findings, the method of attack, the information Bessemer did and did not try to access, and the purported ways in which the reviewer circumvented Fiserv's response to the attack. (Dkt. 1-2 at 45-47; Dkt. 152 (quoting SAC ¶¶ 5, 59, 60, 62, 64-6).) Bottom line: the security reviewer was hired and conducted the attack ***before*** Bessemer made a single claim or allegation and did the very things that give rise to Bessemer's claims and Fiserv's counterclaims.

For these reasons, the Special Master rejected Bessemer's claim that the security review is completely exempt from discovery under the attorney-client and consulting expert privileges. The security reviewer is a fact witness who was an active participant in (and indeed, the perpetrator of) the events at issue. The methods the security reviewer used, the information Bessemer provided to the reviewer in order to facilitate the attack, and the reviewer's observations while conducting the attack are all proper subjects of fact discovery. The Federal Rules of Civil Procedure, along with applicable case law, make that abundantly clear. Fed. R. Civ. P. 26, advisory committee notes; *Pengate Handling Sys., Inc. v. Westchester Surplus Lines Ins. Co.*, 2007 WL 9821901 (M.D. Pa.

Feb. 27, 2007); *Bunzl Pulp & Paper Sales, Inc. v. Golder*, 1990 WL 198151 (E.D. Pa. Dec. 4, 1990). Courts routinely reject attempts to shield an "expert's" conduct from discovery when that conduct is part of what gives rise to the claims at issue. (Dkt. 152 at 3-5 (collecting cases).) And nothing shields the identity of such persons from discovery. (*Id.* n. 2.) That is why the Special Master correctly rejected Bessemer's reliance on authority affording work product protection to post-litigation, after-the-fact investigations in data breach in cases. (Dkt. 216 at 18.) Those authorities have no bearing in cases, such as this one, where the "expert" is the one that attempted the data breach in the first place. (Dkt. 209 at 17-18.)

Moreover, Bessemer's "work product" claims are irreconcilable with its repeated representations to Fiserv and the Court that the security review was performed for ordinary business purposes. When it suited Bessemer's purposes, such as moving to dismiss Fiserv counterclaims, Bessemer argued that the security review was an innocent and legally-compelled exercise, conducted for non-litigation purposes, including auditing and monitoring its vendor and for regulatory compliance. (*See* Appendix A.) It was only ***after*** the Court denied Bessemer's motion to dismiss the counterclaims and ordered discovery that Bessemer's "work product" narrative emerged. Work product, however, does not extend to documents or things created for business, regulatory, or non-litigation purposes. (Dkt. 152 at 5-7 (compiling authority).)

That dooms Bessemer's argument that, because Fiserv was the target of the attack and has certain data and information relating to the security review, Fiserv cannot show the exceptional circumstances required to invade work product. Since the work product doctrine has no bearing here, Fiserv need not show "exceptional circumstances" in any event. But even if it had that burden, Fiserv has demonstrated exceptional circumstances.

Bessemer blithely asserts that Fiserv may only depose Bessemer's CEO to obtain discovery about the security review (without, apparently, any means of impeaching her testimony) and suggests that any other discovery would somehow be "disproportional." But only Bessemer and the security reviewer know the identity of the security reviewer, the instructions and information Bessemer provided to facilitate the attack, the specific methods used, what the security reviewer observed (and did not observe) during the attack, and the resulting analyses and reports. Fiserv does not possess, and has no means to access, that indisputably relevant information; it can be obtained ***only*** through discovery of Bessemer and the security reviewer. Bessemer cannot hide those facts under the auspices of "work product."

A case decided after the initial briefing relating to the security review (but presented to the Special Master), *Twitter, Inc. v. Musk*, is particularly instructive. 2022 WL 3656938 (Del. Ch. Aug. 25, 2022). Presented with remarkably similar circumstances, the *Twitter* court rejected virtually all of the arguments Bessemer advances here. There, Elon Musk sought to terminate a Merger Agreement based on analyses that his data scientists performed, citing their findings throughout his counterclaims. Resisting discovery relating to these same analyses, Musk argued that, as shown by their engagement letters, his counsel retained the data scientists in anticipation of litigation. *Id.* at 3. Analyzing their actual involvement and conduct, the court concluded that the data scientists were also "actor[s] or viewer[s] with respect to transactions or occurrences that are part of the subject matter of [this] lawsuit." *Id.* (citing Fed. R. Civ. P. 26(b)(4)(B) advisory committee's note (1970)). Concluding that Musk relied on the data scientists' analyses to terminate the Merger Agreement and noting that he referenced their analyses throughout his counterclaims, the court held that the data scientists were fact witnesses and that their analyses, documents, and communications were not protected by Rule 26(b)(4)(B). *Id.* at 3-4. The court

likewise rejected Musk's consulting expert and work product assertions under the "exceptional need" standard, permitting the plaintiff to probe the analyses on which Musk himself relied.

Bessemer's passing attempts to distinguish this case are unpersuasive. While the case was decided under state law, the court relied heavily on Rule 26(b)(4)(B), federal case law, and secondary authorities interpreting federal law. *Id.* at n.9-10, 14, 16, 19, 29, 30, 38-39. Likewise, the fact that the experts in *Twitter* were hired pre-litigation presents a distinction without a difference. The work product doctrine applies to documents ***actuall***y prepared for and in anticipation of litigation; that is a substantive, not a merely chronological, analysis. The outcome of that case would not have changed if Musk had merely gone through the perfunctory exercise of serving a praecipe writ of summons before engaging the experts. And, to the extent that Bessemer has grounds to assert work product or other privileges as to specific documents or communications, the Special Master's recommendation permits Bessemer to assert those privileges and log that material for further review and analysis by the parties. The Special Master got it right.

B. BESSEMER'S MOTION FOR PROTECTIVE ORDER ON VOICEMAILS

Bessemer has also refused to produce (and requested to destroy) voicemails that Fiserv left for Bessemer during the security review. Unaware that Bessemer was actually the perpetrator, Fiserv tried multiple times to alert Bessemer to the brute force cyberattack underway. When Bessemer (strangely) did not answer or respond, Fiserv left voicemails. (Dkt. 88 ¶ 42.) Bessemer's intentional lack of response exacerbated Fiserv's damages when Fiserv assumed the attack was malicious. (*Id.* ¶¶ 48, 54.b.) These voicemails are relevant to Fiserv's counterclaims, particularly causation and damages. The Special Master recommended that Bessemer (i) confirm whether it has preserved these voicemails and (ii) if so, produce them. (Dkt. 209 at 9–10.)

As to preservation, Bessemer's litigation hold presumably prevented destruction of voicemails recorded in September 2018—five months after Bessemer filed this case. But, since

filing its protective order motion in January 2022, Bessemer has carefully avoided answering whether it preserved the voicemails. (Dkt. 165.) Its silence is curious: Either Bessemer wants to excuse a failure to preserve the voicemails years ago or it seeks permission to destroy them now. Either way, it has not shown good cause to destroy relevant evidence.

Rather than squarely address the question, Bessemer argues that preserving voicemails is not required under the Court's Model ESI Order. The model order, however, does not prohibit preservation of voicemails. Rather, it directs parties to discuss whether materials such as voicemails are not "reasonably accessible" and to determine whether "the parties agree not to preserve" them. The parties did just that, negotiating an ESI Stipulation that does not waive preservation of voicemails. (Dkt. 122.) Assuming Bessemer has preserved them, the voicemails are relevant. Conceding the point, Bessemer asserts that identifying the voicemails would impose a disproportionate burden. Bessemer has not specified the actual cost or burden of reviewing voicemails from a readily-identifiable, two-day period. Fed. R. Civ. P. 26(b)(2)(B); *see also Bolus v. Carnicella*, 2020 WL 930329, at *6 (M.D. Pa. Feb. 26, 2020) (conclusory statement that producing ESI would require significant expense is insufficient for undue burden). Bessemer has already produced 43 voicemails relating to deconversion. Bessemer wants to cherry-pick which voicemails it will produce in order to avoid discovery about the security review.

Finally, Bessemer argues that production is unnecessary because it admitted to the timing and content of Fiserv's voicemails. Not true: Bessemer's discovery responses evasively state that Fiserv was "attempting to communicate with Bessemer regarding what Fiserv asserted to be potentially fraudulent activity, which was being conducted as a test during the security review." (Dkt. 166-1, RFA No. 25.) Far from confirming what the voicemails said, Bessemer's responses make clear why Bessemer must produce them.

CONCLUSION

For all of the foregoing reasons, the Court should adopt the Special Master's report and recommendation in its entirety and overrule Bessemer's objections.

Dated: July 17, 2023.

Respectfully submitted,

/s/ Jesse L. Byam-Katzman
Efrem M. Grail (PA ID No. 81570)
Brian C. Bevan (PA ID No. 307488)
THE GRAIL LAW FIRM
Koppers Building, 30th Floor
436 Seventh Avenue
Pittsburgh, PA 15219
egrail@graillaw.com
bbevan@graillaw.com
(412) 227-2969

Andrew J. Wronski (*admitted pro hac vice*)
Jesse L. Byam-Katzman (*admitted pro hac vice)*
Foley & Lardner LLP
777 East Wisconsin Avenue
Milwaukee, WI 53202
awronski@foley.com
jbyam-katzman@foley.com
(414) 271-2400

Counsel for Fiserv Solutions, LLC and Fiserv, Inc.